UNITED STATES DISTRICT COURT SOUTHERN DISTRICT OF FLORIDA

CASE NO.: 9:24-cv-80920-AMC

JEFF BUONGIORNO,
Plaintiff,
v.
ALEJANDRO MAYORKAS, et al,
Defendants.

PLAINTIFF'S MOTION TO INFORM COURT REGARDING DYNAMIC IP ADDRESSES AND PRIVACY CONCERNS

Plaintiff Jeff Buongiorno, hereby submits this motion to inform the Court about the nature of **dynamic Internet Protocol (IP) addresses** and how they function in relation to concerns about privacy in public records requests. In support of this motion, Plaintiff states as follows:

BACKGROUND

1. **Dynamic IP Addresses**:

   Most Internet Service Providers (ISPs) assign **dynamic IP addresses** to residential customers. Unlike static IP addresses, which remain constant over time, dynamic IP addresses change periodically. This change is managed through a process called **Dynamic Host Configuration Protocol (DHCP)**, which assigns IP addresses from a pool of available addresses.

2. **Frequency of IP Address Refresh**:

   ISPs frequently refresh and change the IP addresses assigned to residential clients. This can occur every few days, or it may remain unchanged for a longer period depending on the ISP's policies. Additionally, any disruption in the user's network, such as resetting the router or modem, can result in a new IP address being assigned.

3. **Easily Flushed and Reconfigured**:

ISPs can **easily flush and reconfigure new IP addresses** for residential users. This ensures that IP addresses change regularly, reducing the risk of long-term tracking of individuals through IP addresses. As such, the temporary nature of these addresses offers an additional layer of protection for user privacy.

4. **Static IP Addresses and Businesses**:

Static IP addresses—which do not change periodically—are typically assigned to businesses and resolve to traceable entities, such as websites or commercial domains. These static IPs are usually associated with companies or organizations that require a permanent online presence, making them easily traceable. In contrast, residential users typically use dynamic IP addresses, which are less traceable due to their frequent changes.

5. **Privacy Considerations**:

Dynamic IP addresses do not serve as permanent identifiers. The regular refresh of these addresses, along with the ability of ISPs to reset and assign new IPs, significantly diminishes any **privacy concerns** regarding the release of these IP addresses in public records. The temporary nature of dynamic IPs means that they are unlikely to reveal any private or sensitive information about individuals in a sustained manner.

6. **Public Access to IP Addresses**:

Given the nature of dynamic IP addresses, they should not be considered sensitive personal information warranting protection under public records law. Releasing IP addresses, especially in the context of vote-by-mail requests or other election-related activities, does not pose a significant privacy risk due to the frequency of change and the difficulty of linking such information to individuals over time.

7. **National Security Interests**:

It is in the **interest of national security** that the Defendants and their contractors acquiesce to the release of the originating IP addresses for vote-by-mail ballot requests. The integrity of the election process is of paramount importance to the security of the nation, and the release of these IP addresses is necessary to ensure transparency and safeguard against potential threats to election security. This transparency is critical to preventing potential interference or manipulation by malicious actors, whether foreign or domestic.

8. **Judicial Authority to Order IP Flushing:**

Should the Court find any privacy concerns related to the disclosure of dynamic IP addresses, the Plaintiff respectfully reminds this Court that it holds the authority to order Internet Service Providers (ISPs) to flush and reconfigure dynamic IP addresses for residential clients. This action would further mitigate any lingering privacy concerns, ensuring that the temporary nature of these IP addresses is maintained, while still allowing for the necessary transparency in the election process.

CONCLUSION

Plaintiff respectfully requests that this Court consider the nature of dynamic IP addresses and recognize that releasing such information in public records requests does not create a substantial risk to individual privacy. Given that IP addresses are easily reset and reconfigured by ISPs, their use in public records is not a significant privacy concern, and the information should be disclosed to ensure transparency in the election process.

RELIEF REQUESTED

WHEREFORE, Plaintiff respectfully requests that the Court:

1. Acknowledge that dynamic IP addresses are not sensitive personal information.
2. Allow the release of IP addresses in public records requests related to the vote-by-mail ballot process, as such information is necessary for transparency and election integrity.
3. Provide any further relief that this Court deems just and proper.

Dated this Third Day of October, 2024.

Respectfully submitted,

Signed_____

Jeff Buongiorno
Jeff@etektraining.com